TRIP: Coercion-Resistant Registration for E-Voting with Verifiability and Usability in Votegral

Louis-Henri Merino, Simone Colombo, Rene Reyes, Alaleh Azhir, Shailesh Mishra, Pasindu Tennage, Mohammad Amin Raeisi, Haoqian Zhang, Jeff R. Allen, Bernhard Tellenbach, Vero Estrada-Galiñanes, **Bryan Ford**

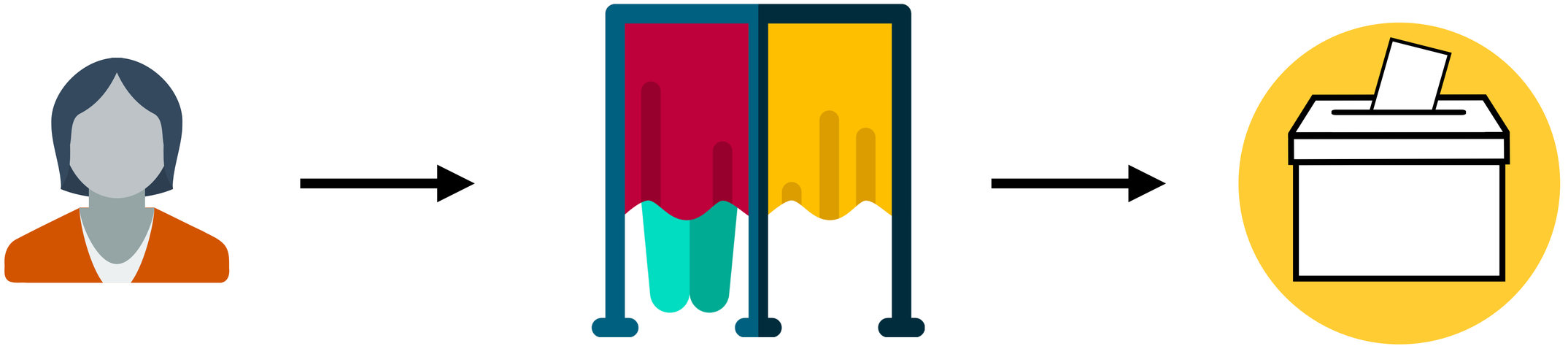
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse
Federal Office for Defence Procurement

EPFL

Massachusetts Institute of Technology

Voting: Essential to Democracy



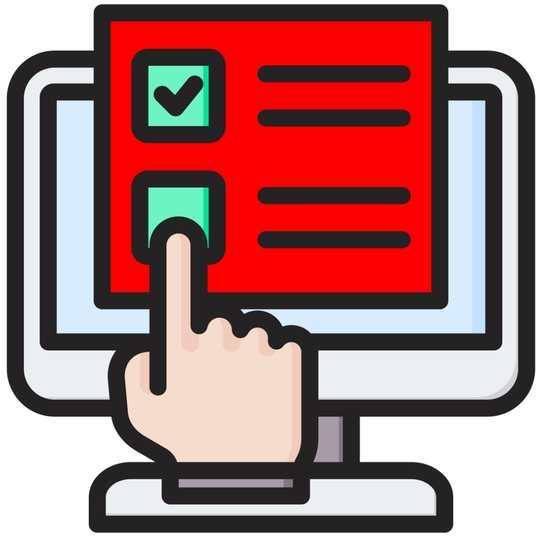
In-person voting via the **Australian Secret Ballot**:
the only approach *globally accepted* for high-stakes elections

Online E-Voting Systems

Home **Hotel**

Cast **votes** on your **own** device from **anywhere**

Online E-Voting Systems



~~Cast votes on your own device from anywhere~~

Cast **a coercer's** vote

Real Examples of Coercion

Election Fraud in North Carolina Leads to New Charges

Saving Democracy: Reducing Gang Influence on Political Elections in El Salvador

October 25, 2024 11:42 CET

By RFE/RL's Moldovan Service

Moldovan Police Accuse Pro-Russian Oligarch Of $39M Vote-Buying Scheme

March 12, 2022

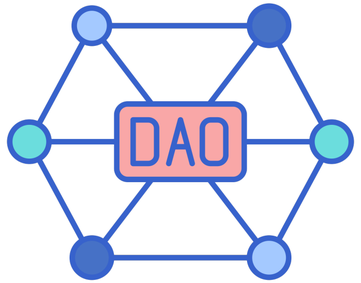
L. McCrae Dowless Jr., a longtime political operative who worked as a contractor for Mark Harris's campaign in North Carolina's Ninth District.

Veasey Conway for The New York Times

Evolving Scalable Coercion Threats

Forceful

Vote-Buying Selfie



"Dark" DAOs[1]
Vote Buying at Scale

Online voting is susceptible to **more scalable** coercion threats

1. Austgen, James, et al. *DAO Decentralization: Voting-Bloc Entropy, Bribery, and Dark DAOs*. arXiv:2311.03530, 6 Nov. 2023.

Talk Roadmap

- **Coercion Resistance via Fake Credentials**
- In-Person Credentialing in Votegral
- TRIP Cryptographic Registration Protocol
- Evaluation: Performance and Usability
- Future Work and Conclusion

Real and Fake Voting Credentials[1]

Real Vote

Intended Vote

Fake Vote(s)

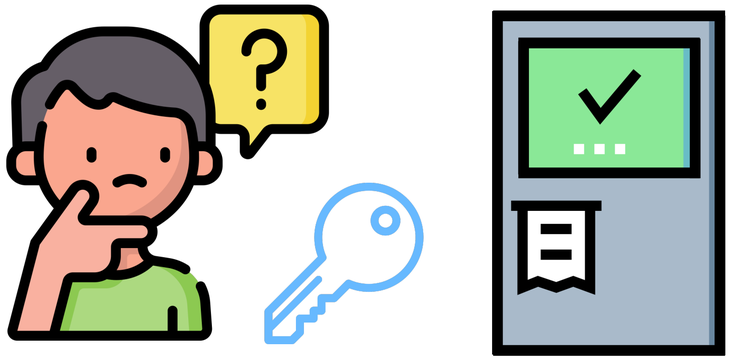
Coerced Vote

Fake credentials cast votes that **do <u>not</u>** count but are **indistinguishable** from **real credentials** which cast votes that **do** count.

1. Juels, Ari, et al. "Coercion-Resistant Electronic Elections." *Towards Trustworthy Elections: New Directions in Electronic Voting*, 2010.

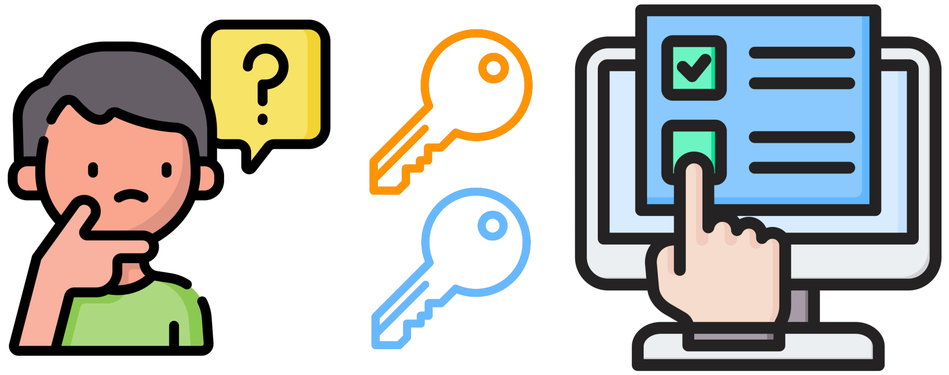
Issues with Fake Credentials

Verifiability



Will My Vote Count?

Usability

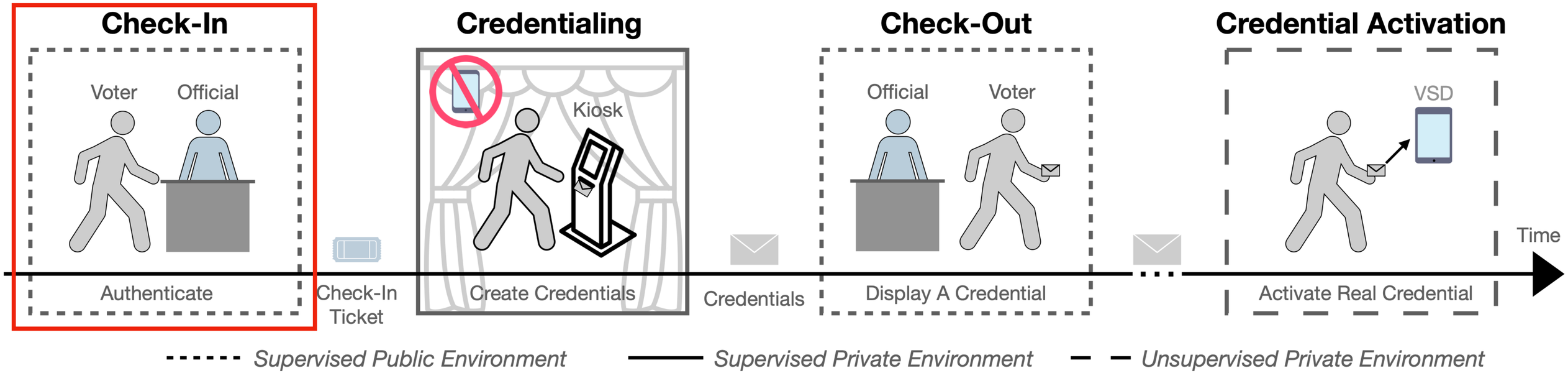


Distinguish Real from Fake?

Talk Roadmap

- Coercion Resistance via Fake Credentials
- **In-Person Credentialing in Votegral**
- TRIP Cryptographic Registration Protocol
- Evaluation: Performance and Usability
- Future Work and Conclusion

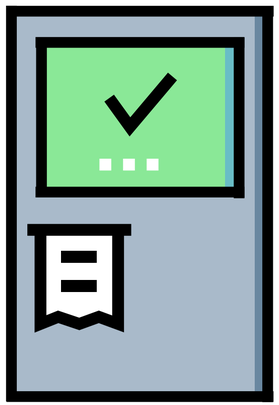
TRIP: Trust-limited Coercion Resistance In-Person



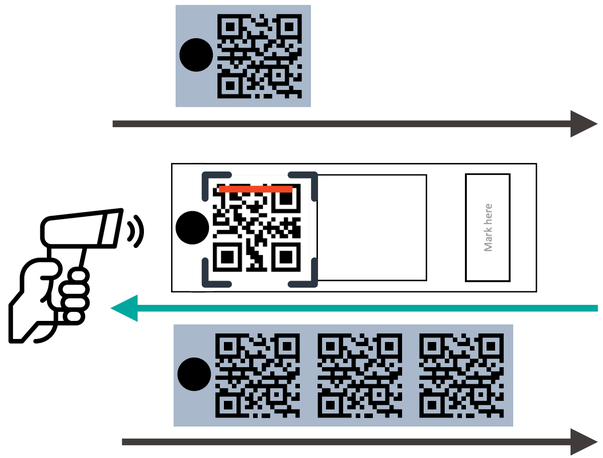
TRIP issues **voter-verifiable real credentials** and **indistinguishable fake credentials**

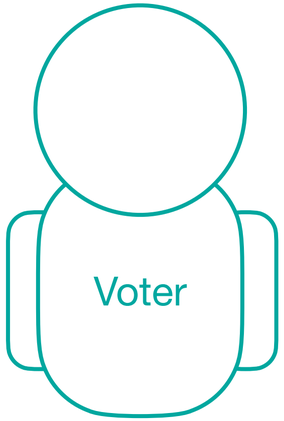
Real Credential Creation Process

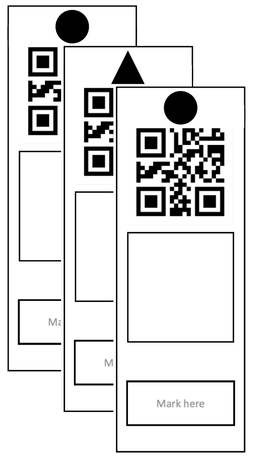
(with an interactive zero-knowledge proof)



Kiosk





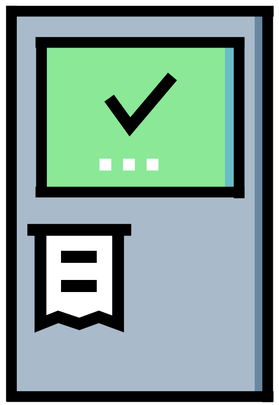


Envelopes

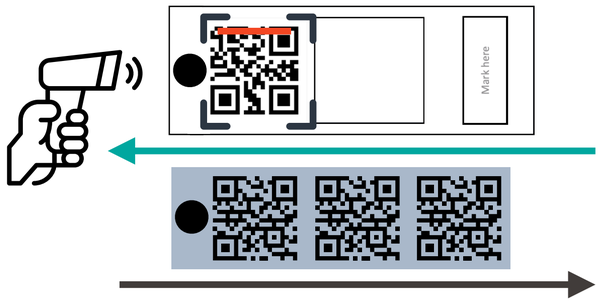
Pen

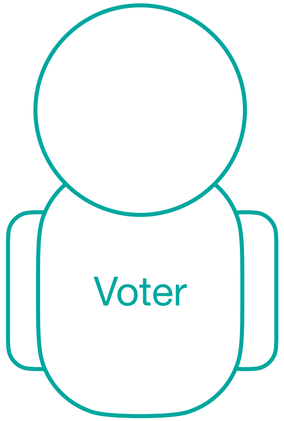
Voter **presents** envelope after kiosk prints **first** QR code

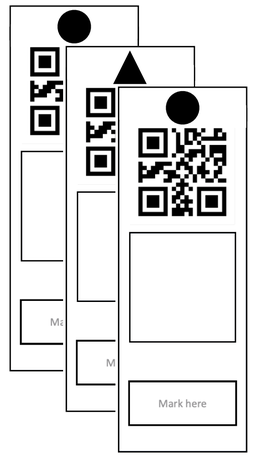
Fake Credential Creation Process



Kiosk







Envelopes

Pen

Voter **presents any** unused envelope

Talk Roadmap

- Coercion Resistance via Fake Credentials
- In-Person Credentialing in Votegral
- **TRIP Cryptographic Registration Protocol**
- Evaluation: Performance and Usability
- Future Work and Conclusion

Under the hood…

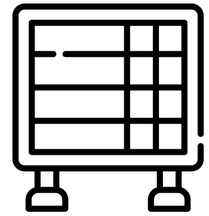
What **cryptography** is happening?

- Which voters *need not* understand

Registration Log

Credentialing in Booth

Public Ledger



Alice

Real: R_A

Fake: F_{A_1}

Fake: F_{A_2}

...

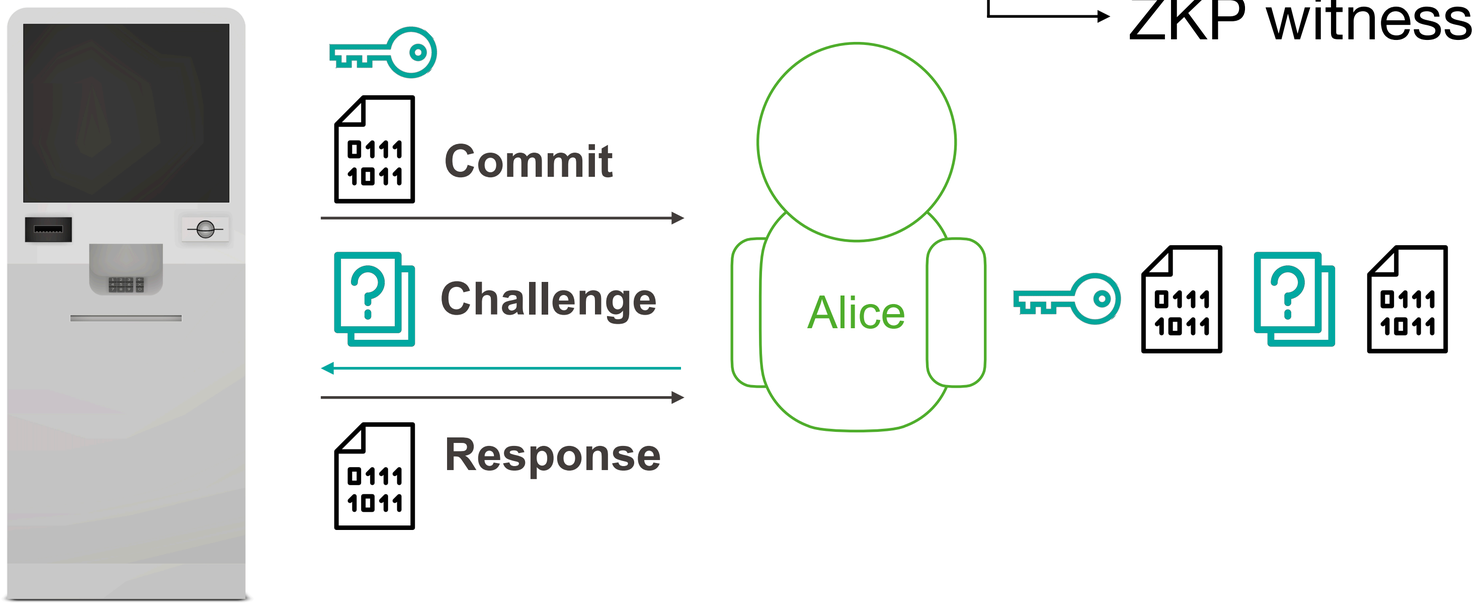
Alice	$T_A = \text{ElGamal}(R_A, x_A \in Z_q)$
Bob	$T_B = \text{ElGamal}(R_B, x_B \in Z_q)$
Carol	$T_A = \text{ElGamal}(R_C, x_C \in Z_q)$

Real Credential Issuance
Schnorr interactive zero-knowledge proof

Convince **Alice** T_A (on public ledger) is an ElGamal encryption of R_A (given to Alice)

$$T_A = \text{ElGamal}(R_A, x_A \in Z_q)$$

ZKP witness



➕ Kiosk forced to give the voter their real credential

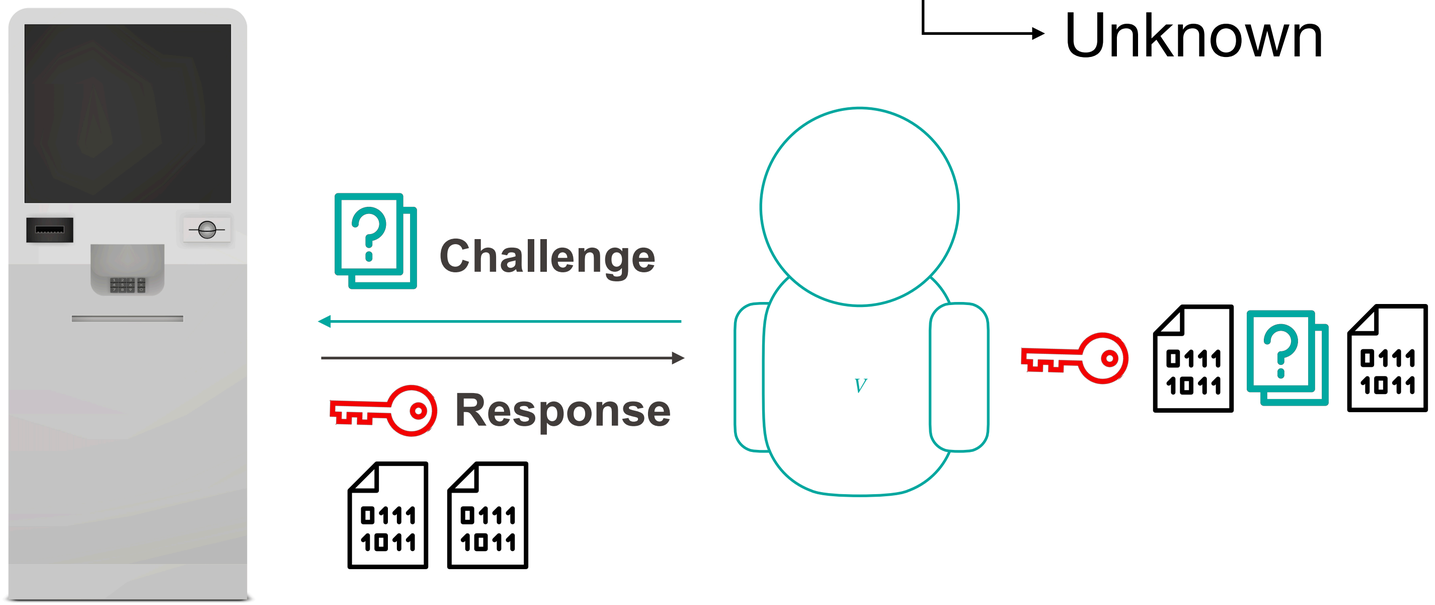
➖ Cannot create fake credentials using this process

Fake Credential Issuance

Simulated Schnorr interactive zero-knowledge proof

Falsely prove for **Alice's coercers** that T_A is a correct ElGamal encryption of F_A

$$T_A = \text{ElGamal}(F_A, \underbrace{x \in Z_q}_{\text{Unknown}})$$

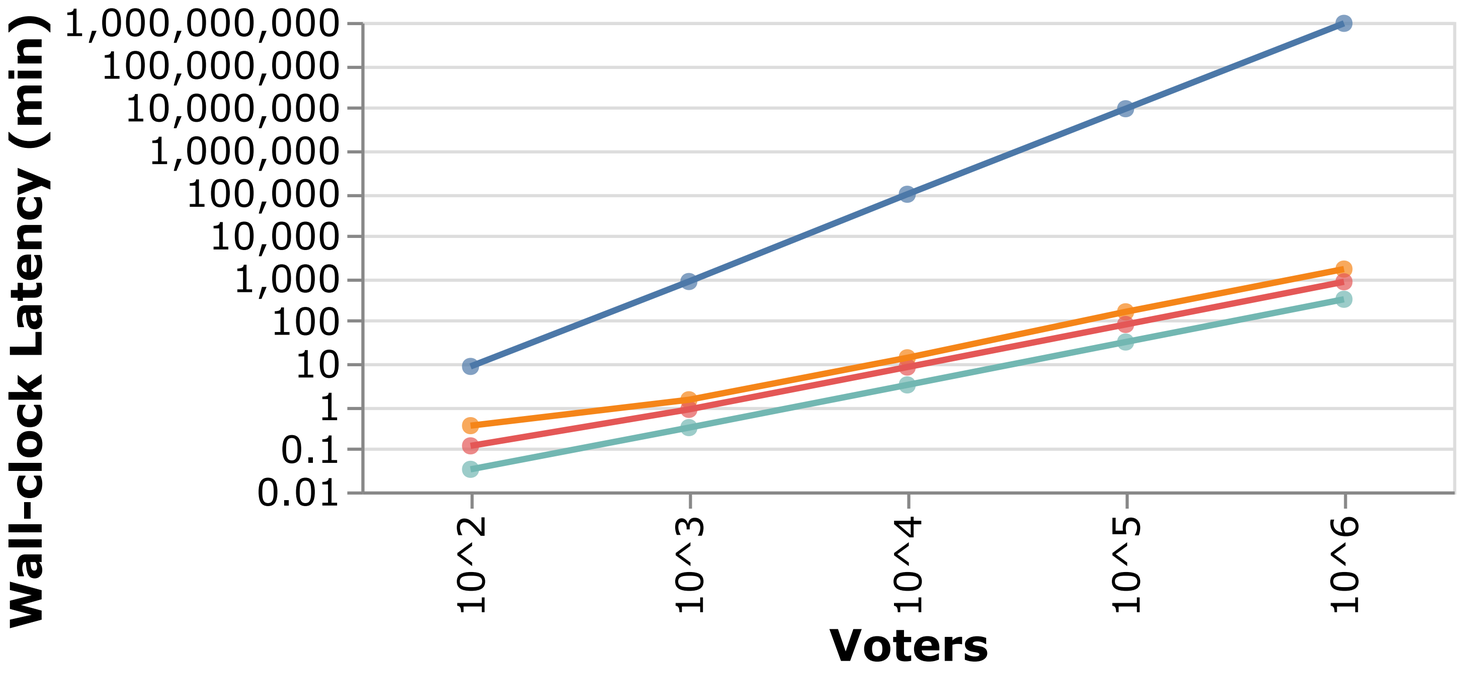


- Real and fake credentials *indistinguishable* outside privacy booth
- Voters distinguish real and fake credentials at creation (3 vs 2 steps)

Talk Roadmap

- Coercion Resistance via Fake Credentials
- In-Person Credentialing in Votegral
- TRIP Cryptographic Registration Protocol
- **Evaluation: Performance and Usability**
- Future Work and Conclusion

End-to-End Coercion-Resistant Verifiable E-Voting System



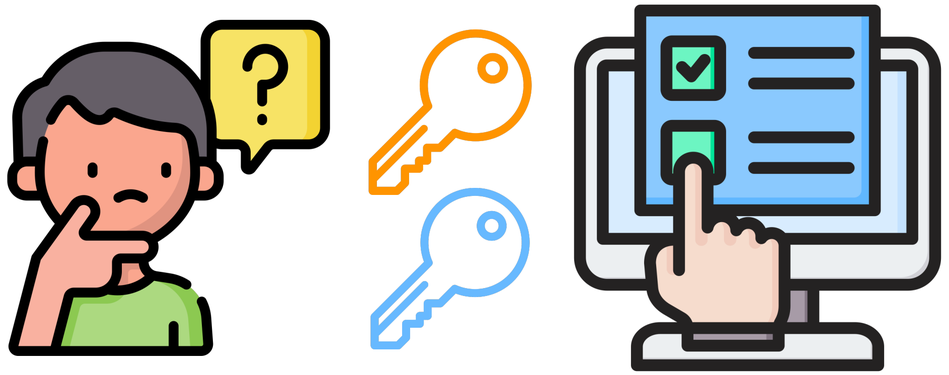
System
- Civitas
- SwissPost
- VSYS-Tally
- VoteAgain

- **1 million voters**
  - Civitas: 1,768 years
  - Swiss Post: 27 hours
  - **Votegral: 14 hours**
  - VoteAgain: 5 hours

- Votegral achieves **comparable latency** to the state-of-the-art voting systems
- Votegral **significantly outperforms Civitas**, the closest comparable system

Usability

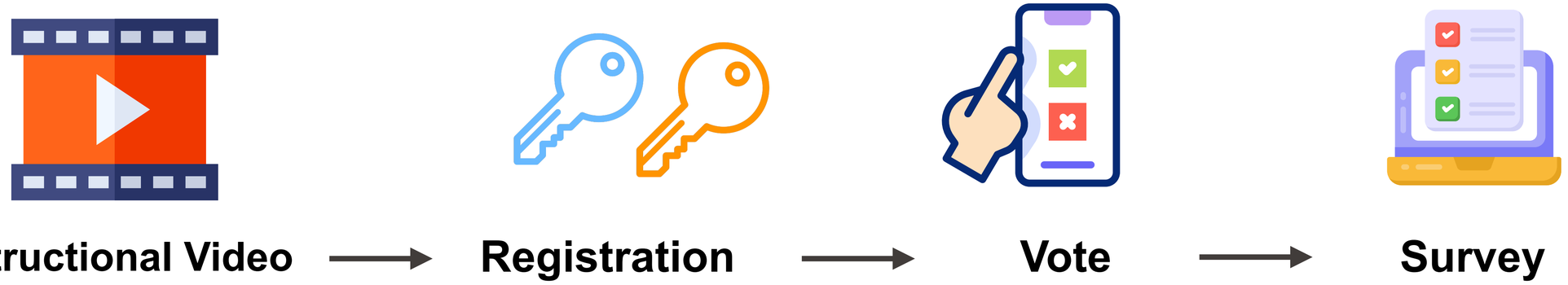
Comprehension?



Distinguish Real from Fake?

User Study

- 150 participants
- Suburban Park in Boston, Massachusetts, U.S.A.



~30 min per participant

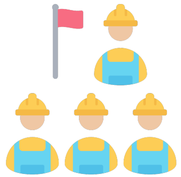
Is Coercion a Perceived Problem?

26%

report experiencing or knowing of someone who has experienced at least one form of voter coercion

Reported Sources

Spouse



Labor Unions

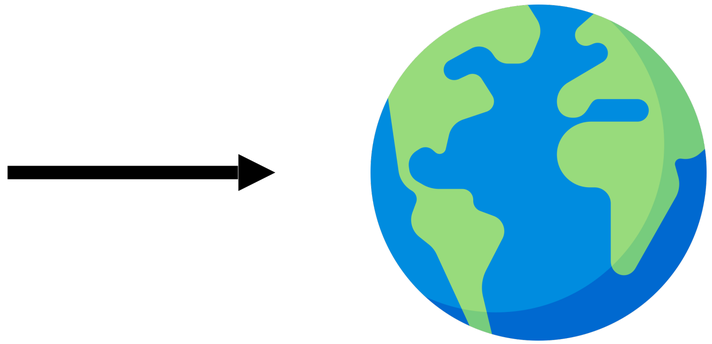
Colleagues

Party Members

Are Fake Credentials Comprehensible?

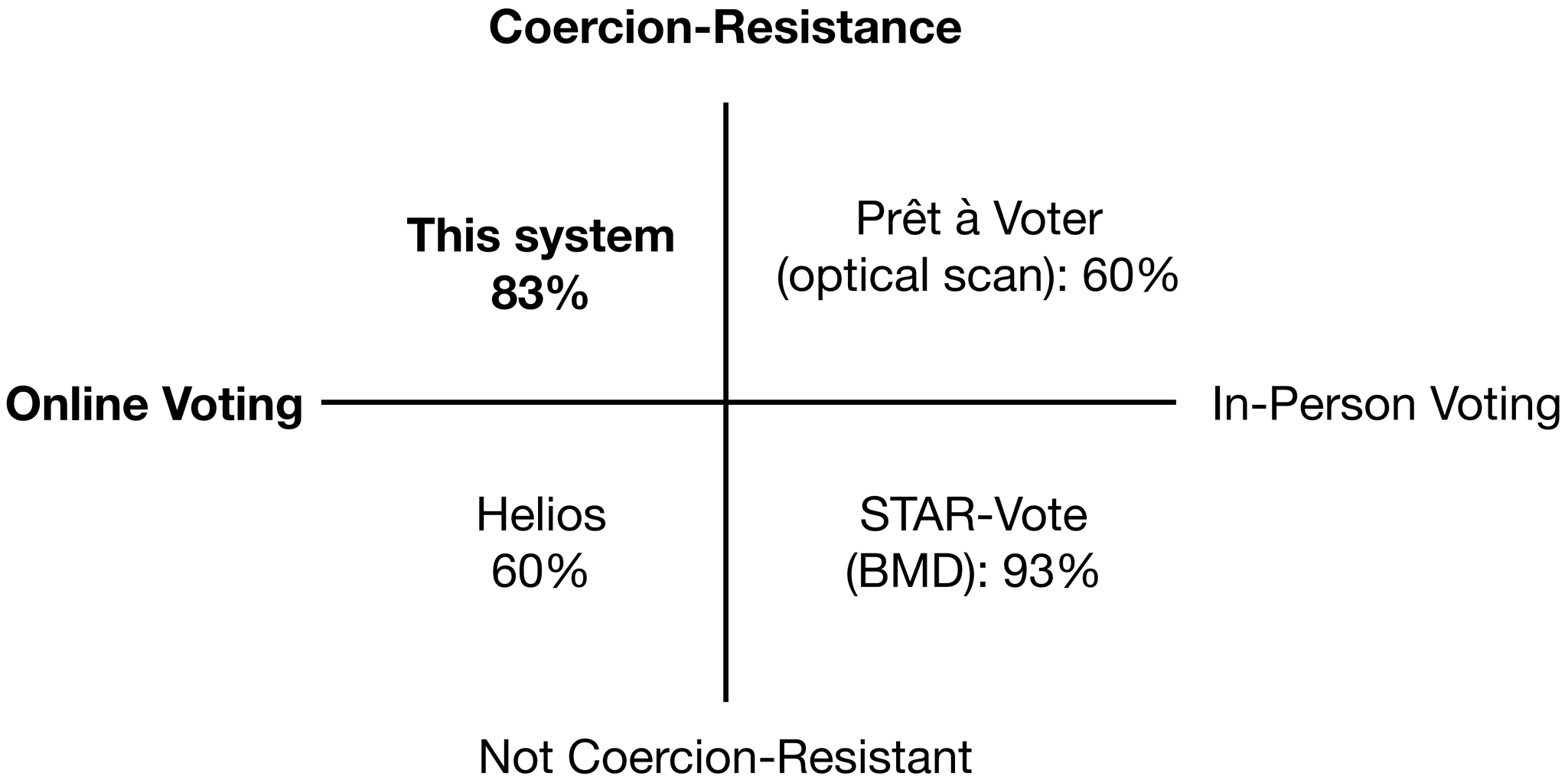
96% understood their use

76% created a fake credential



53% would create in real situation

Comparative System Usability



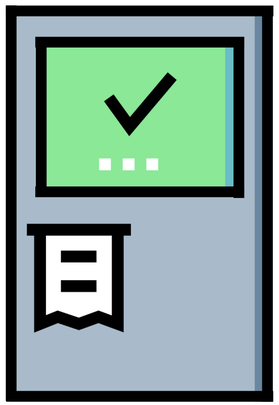
Acemyan, Claudia Z., et al. *Usability of Voter Verifiable, End-to-End Voting Systems: Baseline Data for Helios, Prêt à Voter, and Scantegrity II*. no. 3, 2014.
Acemyan, Claudia Ziegler, et al. "Summative Usability Assessments of STAR-Vote: A Cryptographically Secure E2e Voting System That Has Been Empirically Proven to Be Easy to Use." *Human Factors*, vol. 64, no. 5, Aug. 2022

Successful Creation and Use

Comprehension

96%

Create Credentials



95%

Activate Credential

92%

87%

Vote with Real Credential

90%

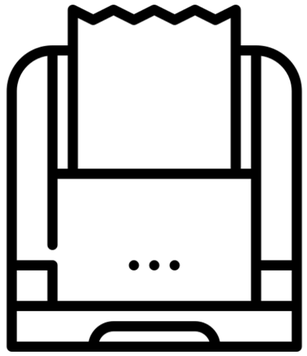
83%

Talk Roadmap

- Coercion Resistance via Fake Credentials
- In-Person Credentialing in Votegral
- TRIP Cryptographic Registration Protocol
- Evaluation: Performance and Usability
- **Future Work and Conclusion**

Limitations & Future Work

- Side Channel Attacks



Printer Noise

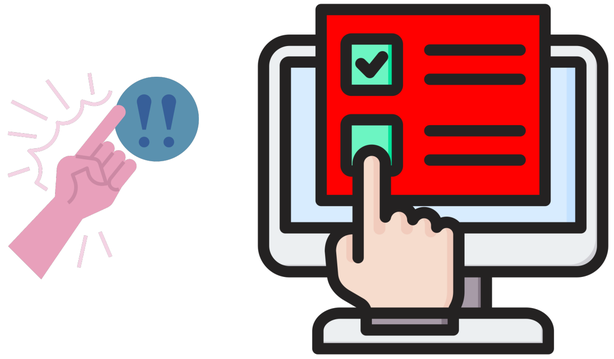
Timing Attacks

Electromagnetism

- Need Post-Quantum Security
- Need Hardened Implementation (e.g., Formally Verified)

Conclusion

Coercion Problem



TRIP Credentialing

Real Credential
(Non-Transferable Proof)

Fake Credential
(False Proof for
Coercion-Resistance)

TRIP Usability

STAR-Vote: 93%

Online Voting

TRIP
83%

Helios: 60%

Prêt à Voter: 60%